Bluetooth Security Analysis for Mobile Phones

João Alfaiate, José Fonseca
UDI – Research Unit for Inland Development of Guarda Polytechnic Institute, Portugal
jc.alfaiate@gmail.com, josefonseca@ipg.pt

***Abstract*— Mobile devices are becoming more and more omnipresent due to their lightweight, small size and increasing performance. Almost every mobile device has Bluetooth (BT) capabilities and this powerful combination widely used in our daily life is coming to new environments like the car and the military industries. As any technology, BT has security issues that hackers have extensively exploited over the years, while users seem not to care too much. To raise the security awareness we present an analysis of BT attack methods and tools over time. We paid particular attention to the severity, possible targets and the ability to persist over new versions of BT. Results show that adversaries can take complete control of the victims' mobile device features if they forget to use simple safety measures like turning off the BT when not in use. To increase security we also propose the development of a novel BT Firewall.**

Keywords-Mobile Phones, Security, Hack, Attack, Bluetooth.

I. INTRODUCTION

Mobile phones are increasingly becoming omnipresent in our lives. They evolved from simple devices that could only be used to make phone calls and send short text messages to fully featured miniature computers. Nowadays, they are capable of browsing the Internet, read and send emails, edit documents, perform complex calculations, synchronize calendars and to-do lists, take photos, make videos, play games, and much more. This may justify the 6 billion mobile phone users, representing 87% of the world population [1].

The huge adoption of mobile phones followed the implementation of new developments in technology. One such technology that plays an important role is Bluetooth (BT) that is used to share contacts, create personal networks, hands-free communication, and much more.

The growing acceptance of mobile devices and their new features allowed them to invade markets that were not foreseen when they were first developed. Evidences of this can be found in the car industry, the military [2], all sorts of multimedia, advertising, and in daily tasks like e-Commerce and e-Banking [2]. Nevertheless, every time a new technology reaches the masses like this, it also calls the attention and the interest of malicious minds that want to exploit this new opportunity on their benefit.

In this paper, we present a study analyzing the BT presence in mobile devices, focusing on their security problems. We address this important aspect by analyzing common mobile attacks using BT and how to prevent them. We paid special attention to the most critical security problems affecting BT, which are BlueSnarf, BlueSnarf++ and BlueBug.

BT is a common entry point for many attack methods in mobile phones, and the information presented in this paper can be useful to educate and raise the awareness of mobile users in order to follow best practices. Using the right application configuration and simple things like turning off BT when not in use is essential to avoid the possibility of attacks. With over than 70% mobile phones with BT, they should offer a more reliable protection to their users [3]. In fact, security should not be pushed back to users and a mechanism should exist to prevent undesired access. This is why we also propose the development of a BT Firewall, which from the best of our knowledge does not exist yet.

The remaining of this paper is organized as follows: Section II presents the BT evolution over time. Section III details the BT security features. Section IV provides a study on BT attack methods and tools. Section V presents an example of a BT attack and the proposal of a BT Firewall. Section VI concludes the paper and introduces future work directions.

II. BLUETOOTH EVOLUTION

Since the first public version of BT in 1999, five updated versions were released until 2010. They are shown in Table I, along with the most relevant features for our study [4, 5].

TABLE I. BLUETOOTH FEATURES

Bluetooth Versions	Year	Faster connection	SSP	Security Mode 4	Bug fixes	Error detection	Synchronization	Data Rate	L2CAP	HCI for AMP	Security for AMP	Power consumption
1.1	2002				X							
1.2	2003	X				X	X					
2.0	2004							X				
2.1	2007		X	X								X
3.0	2009							X	X	X	X	X
4.0	2010											X
		New Features			**Enhancement Features**							

The most relevant BT enhancements were provided by the following versions:

- **Version 2.1**: Security aspects.
- **Version 3.0**: Enhanced Data Rate (EDR), which provides more speed and improved battery life.
- **Version 4.0**: Low power consumption.

PEst-OE/EGE/UI4056/2011 – project financed by Science and Technology Foundation

Data speed is a common concern and has been addressed in almost every version. The latest versions (2.1, 3.0 and 4.0) have a huge concern on power consumption, which is crucial for mobile devices. However, important security aspects were only effectively addressed with version 2.1 in 2007, eight years after BT was first released.

The following sub-sections provide details on data speed and the usage of BT in mobile phones, e-Business, car industry, and in the military. Because of its importance, security is addressed in its own section III.

A. *Data speed and radio ranges*

Since the release of BT, many manufactures used its reasonable data transfer rate ability for a wide range of purposes, such as printers, cameras, mobile phones (Personal Digital Assistance and Smartphones included), notebooks, among others.

Initially, BT started with 1 Mbps data rate and increased to 3 Mbps in version 2.0. However, the biggest leap occurred in version 3.0 allowing up to 24 Mbps, which was an 800% enhancement.

For the proper utilization of the device, these transfer rates are very important, but is also very important the distance range that can be reached. BT is divided in three radio ranges [5, 6]:

- **Class 1**: approximately 100 meters (300 feet).
- **Class 2**: approximately 10 meters (33 feet).
- **Class 3**: approximately 1 meter (3 feet).

B. *Bluetooth in mobile phones*

BT is used in many of our daily personal objects, but the most used scenario is probably for mobile communications. Mobile phones grew to be the best market for BT devices. With over than 70% of BT enabled devices being mobile phones [3] Nokia seems to lead the market share [7].

This major mobile boom allowed BT to increase its shipment in a yearly basis. Today, over than one billion BT devices are in use worldwide [8], and by the year 2013 the shipments expect to exceed 2 billion [9].

C. *Bluetooth in the car industry*

In some countries it is against the law to use a mobile phone while driving a car [10], but using a wireless system to communicate with a mobile phone is legal since the driver has both hands free. The car industry is quite interested in BT and many vehicles have BT capabilities. The following list details some features specifically developed for cars:

- Nokia Research Center presented a solution that allows the control of several electronic media systems of the car using BT [11]. The car displays the phone's applications and the driver can control them either by voice or by touch screen.
- Parrot SA presented an Android based head unit (the hardware component that interfaces electronic media systems with the car) that includes hands-free BT [11, 12].
- The Ford motor company in collaboration with Microsoft launched Ford SYNC, which is capable of connecting to any mobile phone or digital media player with the car itself [13].

D. *Bluetooth in the military*

The military has several projects that actually use BT as the communication protocol. Some examples are [2]:

- The Defense Advanced Research Project Agency (DARPA) with their wireless mesh network for the LANdroids project.
- The Air Force Research Laboratory (AFRL) for their group of miniature helicopters connected by BT.
- The Space and Naval Warfare Systems Center with their mobile robot which uses BT.

However, BT features and its ease of use can also jeopardize the security of the devices. For example, the US Navy tested a recruiting method using the BT data transfer ability. In 13 key locations with a population of 11,000 BT devices, the Navy could anonymously transfer videos to 18% of such devices [2]. If it was possible to send video it would also be possible to send any other file with malicious intentions.

When data transfer or third party resource access is necessary, security should be a top concern. This is discussed in the next section.

III. BLUETOOTH SECURITY

The worldwide spread of mobile phones with BT and the decision to use it in situations not foreseen when the BT protocol was developed, attracted the attention for security problems. To address these security problems, in 2007 BT version 2.1 (the fifth release) had more security features than all the other versions, affecting a huge number of security related aspects [4]. Below are the most relevant:

- **Encryption Pause and Resume**: This feature pauses the encryption when the link key connection needs to be changed and when the master and slave roles of the devices need to be switched. After these changes, the encryption resumes.
- **Secure Simple Pairing (SSP)**: Created to simplify the pairing process and improve the BT security. The two main security aspects are to protect against passive eavesdropping and man-in-the-middle attacks. It uses the Elliptic Curve Diffie Hellman (ECDH) public key cryptography as a means to prevent passive eavesdropping attacks.
- **Security Mode 4**: Used for SSP.

BT is still one of the causes of security problems in mobile phones, in spite of the updates released. Even BT version 2.1 mostly devoted to security, still seems to leave some security problems unsolved. According to Andrew Lindell, chief cryptographer for Aladdin Knowledge Systems Ltd, SSP in version 2.1 has specification bugs allowing man-in-the-middle attacks [14]. For example, the six random digit password used in paring the devices can be obtained within 10 attempts. BT has four security modes to pair devices [6]:

- **Security Mode 1** allows unsecured links.

- **Security Mode 2** procedures are executed after the link establishment. This is a service level enforced security where BT service security can be configured to use authentication and authorization, authentication only, or open to all devices.
- **Security Mode 3** initiates link-level security before the physical link is fully established.
- **Security Mode 4** is a service level security mode where the link-level connections are initiated only after link setup, but with added security due to the SSP. This mode is mandatory for all BT versions after 2.1 inclusive, but Security Mode 2 is used instead when the remote device does not support SSP.

The National Institute of Standards and Technology (NIST) consider Security Mode 3 as the strongest, due to authentication and encryption establishment requirement before the physical link is established [6]. To keep software that uses BT secure, organizations are advised to use the strongest security mode available for BT devices (Security Mode 3).

IV. BLUETOOTH ATTACK ANALYSIS

This section presents BT security problems, and describes the most common procedures used to exploit BT vulnerabilities.

During our research, we found 6 tools and 11 methods to attack BT. Table II shows the attacks in a chronological point of view according to the year of discovery. We can verify that the majority of the attacks appeared between years 2004 and 2007. This timeframe corresponds to the upgrade of BT from version 2.0 to 2.1, which took three years to be released.

TABLE II. BT ATTACK PROCEDURES

Year	**Attack procedure**	**OS**		***Tool***	***Method***
		Linux	***Windows***		
2001	BTScanner	X	X	X	
2003	BlueSnarf				X
	BlueJacking				X
2004	Blooover	X	X	X	
	BlueBug				X
	BlueSmack				X
	Bluetooone				X
	BlueSniper				X
	Blueprinting				X
2005	BlueSnarf++				X
	HeloMoto				X
	Crack PIN				X
	Car whispering	X		X	
	HIDattack				X
2006	BackTrack	X		X	
	BlueScanner		X	X	
2007	BTCrack		X	X	

From Table II we can verify that there are many ways to attack a BT device. We verify that the three most recent procedures are Tools, and two of them were designed for the Windows Operating System (OS). Developing this type of software for Windows users, highly increments potential attacks since Windows is by far the most common OS. The Blooover tool runs both in Linux and Windows because it was developed in Java.

To better analyze the impact of BT attacks, their real threats need to be understood. Table III shows information that can be obtained by attacking BT, which can be used for many types of attacks. For example, to perform a BlueBug attack, the BTScanner or the hcitool (a BT configuration utility present in many Linux distributions) can be used to obtain the necessary information from the target devices.

TABLE III. DEVICE INFO OBTAINED BY ATTACK PROCEDURES

Attack procedure	**Device Info**					
	Address	***Class***	***Name***	***Type***	***PIN***	***Services***
BTScanner	X	X	X			
hcitool (Linux tool)	X	X	X			
Blueprinting	X					
BlueScanner	X			X		X
BTCrack					X	

Table IV shows the impact caused by various attack procedures. Although most of the procedures are directed at a single objective, their inner workings are complex. The following list describes the impacts mentioned in Table IV:

- **SDP**: Allows the discovery of the services enabled and their characteristics.
- **OBEX**: Eases the exchange of binary objects between devices.
- **Security Audits**: Measures technical assessment of a system or application.
- **Send vCards**: Sends messages to other BT devices.
- **Send AT commands**: AT commands are used to control the communication system of the device.
- **DoS attack**: Intends to make the device resources unavailable.
- **Check known vulnerabilities**: Performs an audit on mobile phones to verify whether they are vulnerable to a set of known issues.

The attack impacts shown in Table IV are quite different from each other and it is important to identify which attack is more critical in what concerns the access to private information or full control of the device. For example, the ability of BlueJacking to send text messages to another device seems harmless compared to the ability of BlueBug to send AT commands.

TABLE IV. IMPACT OF ATTACK PROCEDURES

Attack procedure	**Impact**						
	SDP	***OBEX***	***Security audit***	***Send vCard***	***Send AT commands***	***DoS attack***	***Check known vulnerabilities***
BTScanner	X	X					
hcitool	X	X					
sdptool	X						
BlueSnarf		X					
BlueJacking		X		X			
Blooover			X				X
BlueBug					X		
BlueSmack						X	
BlueSnarf++		X					
HeloMoto				X	X		

The most relevant attack procedure affecting BT are:

- **BlueSnarf**: Consists on connecting to the OBEX Push Profile (OPP), which allows an easy exchange of files. Since most cases of OPP do not require the service authentication, a weak OBEX implementation may be the entry point for an attacker [2, 15]. If an attacker connects to OBEX and performs an OBEX GET request, files such as the phone book, pictures, or even the calendar can be obtained. More dangerous, is an improper device firmware implementation where an attacker can actually obtain any file, if the name of the file is known.
- **BlueSnarf++**: Is an enhancement of the BlueSnarf, allowing the attacker to also have full read and write access to the device's file system when connected to the OPP [15]. To succeed, this attack requires that the device runs on an OBEX FTP server and can connect to an OBEX Push service without pairing.
- **BlueBug**: Is a name given to a BT vulnerability present on some mobile phones, allowing remote AT commands to be executed on target devices [2, 15]. An attacker exploiting this can obtain information from the mobile phone or even take complete control of the device. This attack can be performed in few seconds, and allows for example, to make a phone call, send and read SMS messages, access and edit the phonebook, forward calls, connect to wireless networks, and change the phone's service provider.
- **BlueJacking**: Consists on sending anonymous vCards (business cards) or text messages to other devices through OBEX, which seems to be physically harmless.
- **HeloMoto**: Is a combination of the BlueSnarf and the BlueBug attacks. The origin of the name is due to a security breach found in some Motorola phones [2, 15].

The two procedures that can actually send AT commands and remotely control the device are BlueBug and HeloMoto. The HeloMoto may not be a widespread attack since it only affects some mobile phones from Motorola. The BlueBug attack seems to be more dangerous since it can be executed on devices from several brands. The brand names are not publicly available because the Trifinite group, who identified this leak, only discloses this information to device manufacturers [15]. Besides the type of information already mentioned that attacks can obtain, access to personal information stored in the mobile phone is also possible. This is a major issue since private data can be traded in the underground market around the globe [16].

In spite of the efforts made to secure and patch BT from the specification, it is still one of the most relevant causes for security problems in mobile phones. Being BT a wireless connection technology, mobile phone users cannot really "see" or "feel" BT and may not be aware of the dangers in case of a security breach. It is estimated that 73% of mobile users are unaware of critical attack types (like BlueSnarf, BlueBug, and Bluejacking) and the damage they may inflict, according to InsightExpress [17, 18].

Moreover, attacks to BT devices can target millions of possible victims. This occurs when the vulnerability affects a widespread device, like the iPhone that accounts for 51.15 million devices worldwide [19]. For this widespread device, a BT vulnerability was discovered in the Service Discovery Profile (SDP), which allows the discovery of enabled services and their characteristics [2]. The attack uses the SDP features to send a maliciously crafted message allowing the attacker to access the root shell of the device.

The discovery of BT security problems is not only of the interest of attackers, but it is also part of the research done for this technology to continue growing as a safe and reliable wireless option. One major player investing their resources to discover BT security failures is The Trifinite Group [15]. Like other common security vulnerabilities (for example, the buffer overflow in desktop and mobile applications), there are many methods and tools to exploit BT devices (like those presented in Table IV).

V. BLUETOOTH SECURITY PROPOSAL

Given that BT weaknesses are known for some years and BT security has also been improved, we wonder how safe the BT devices are.

To verify the easiness and the assets put in danger by attacking BT we have made the following experiment: we associated an attack machine as a trusted BT device of a mobile phone (this is a standard procedure when connecting together two BT devices) and we tried to execute AT commands. In a real situation this acceptance as a trusted device can be achieved through social engineering, spoofing of other trusted devices, etc. The main idea of this experiment is to expose what an attacker could do with the phone using this simple procedure. Recall that the procedure used is the basis for any of the BT attacks described in the previous section.

A. Attack procedure

The procedure used in our attack was based on the BlueBug attack. The machine used for the attack had Ubuntu Linux 8.04 Operating System installed. As target devices, we used two Nokia mobile phones as shown in Table V. Table V also shows the need to manually accept (or automatic bypass) a connection from a previously known BT device.

TABLE V. MOBILE PHONES ATTACKED

Mobile phone	Launch year	BT version	Connection bypassed if device paired
Nokia 3110 classic	2007	v2.0	No
Nokia 6303i classic	2010	v2.1	Yes

Before going any further we can see an important difference in the way the phones deal with the pairing of previously associated devices. While the Nokia 3110 classic needs the user to accept (or deny) the incoming BT connection, the Nokia 6303i classic bypasses the authorization and accepts all trusted devices by default. If an

attacker is able to make a rogue device to be associated by the target phone he will be able to attack the phone at any time without being noticed.

The following four steps show the procedure executed from the Linux Shell of the attack machine, as root:

1. **# hcitool scan** – searches for the MAC address of the target BT device.
2. # **rfcomm connect 0 [Target Mac Address] 1** – connects to the target device by RFCOMM.
3. **# minicom –s** configure **A- Serial Device : /dev/rfcomm0** – configures the target device to emulate RS-232 serial ports in order to start a communication.
4. The attacker is ready to send AT commands to the target BT device.

B. *Attack results*

After establishing the RFCOMM to both mobile phones, they were ready to execute the AT commands issued [20]. Table VI shows some AT commands executed, just to have a sample of what was possible to achieve. Recall that AT commands allow executing not only most of the communication functions, but also many other functions to control phone features as the access to the phonebook.

TABLE VI. AT COMMANDS EXECUTED DURING THE ATTACK

AT Command	Description
CGMM	Request ME Model Identification
CMGF	Message Format
CPMS	Preferred Message Storage
CPBR	Read Phonebook Entries

We can see that a trusted BT device can execute a variety of AT commands. It seems that there is no control over it. Our results are corroborated by other studies. To analyze how many BT users could be victim of an attack, a study in London concluded that from 943 mobile phones, 40% had their BT default settings. Moreover, 138 of them were proven to be vulnerable to BlueSnarf attacks [21]. Another test done at the CeBIT technology fair in Hannover concluded that from a range of 1,300 devices, 50 devices were vulnerable to the BlueBug attack [15].

C. *Bluetooth Firewall Proposal*

In our mobile world, BT devices are an easy target for an experienced hacker. Since BT can be used in many daily tasks, it is common practice to have configured in our mobile phone several trusted devices for advertising campaigns [22, 23]. This is a real threat and increases the probability for an attack, if there is no other mechanism to filter BT connections. To reduce the risk of being attacked, users of BT devices should follow best practices, like:

- Turn BT off when not in use.
- Change the default security settings to a more restrict mode whenever possible.
- Remove trusted devices that will not be used.

Not surprisingly, the best protection is turning off BT, but this prevents the use of this wide spread and useful technology. Moreover, all of these practices move the security actions to the user, which is considered by many security practitioners as a bad option. The device should be secure by default, allowing the most important tasks to be done safely, with the least user intervention.

To achieve this kind of filtering and protection on the BT part of the device, we propose the development of a BT Firewall. It could be used to protect against the majority of known attacks, as well as new ones that may appear and use the same entry point. The BT Firewall could as well have a white list and a black list of rules, which can be used to filter devices that should or not be associated with the phone.

The BT Firewall should protect the RFCOMM protocol, which is the second protocol layer on the host side of the BT protocol stack [24], as shown in Fig. 1. By protecting this protocol, all connections that use OBEX, TCP, or intended to send AT commands, could be filtered.

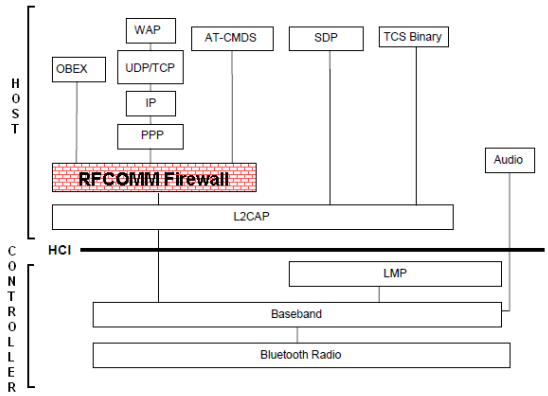

Figure 1. Bluetooth Protocol Stack with the Firewall

The proposed BT Firewall may also have the ability to group user profiles into three main categories (Temporary, E-Commerce and @Home, for example), filtering which BT devices have access to its matching profile (Fig. 2).

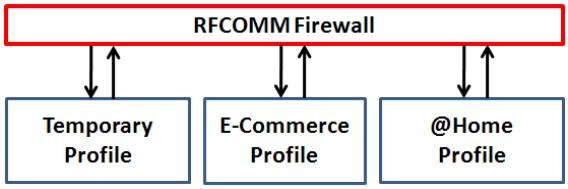

Figure 2. Main User Profiles

The @Home profile is for all the devices used in our daily tasks, which should be well known and thus may have a higher level of trust. The Temporary profile is for any type of connection not regularly used and should have a high security restriction. The E-Commerce profile is for BT trading and should have very specific features. We consider that this level of protection in the E-commerce may help potentiate this important streak since this is an area far from being explored yet.

When a new BT device tries to connect, the Firewall will prompt to the user to accept or deny the access, along with the option to associate the connection to a profile. The

Firewall will filter MAC addresses, the Universally Unique Identifier (UUID), and the server channel identifier (in case of a client connection), identifying the BT device to its respective profile. The Firewall may also have a black list of undesired connections.

To achieve security independency between profiles, the same BT device cannot belong to more than one profile. The Firewall will also be responsible for monitoring the traffic and alert the user in case of suspicious actions. BT Firewall filter definition may be updated regularly as soon as new signatures are provided.

The ability of the BT Firewall to authenticate connections by user profiles is a novel approach to protect BT users. Other approaches focus on specific problems, like the protection against malware propagation, using the Blue-Watchdog [25], or improving the already provided encryption of the communication [26]. These approaches are, however limited in the scope, and do not provide the holistic protection that a BT Firewall is capable of.

VI. CONCLUSIONS

In this paper we analyzed BT security and the most common attack procedures: BlueSnarf, BlueSnarf++, and BlueBug. The BlueSnarf and BlueBug attacks are capable of obtaining private information such as the calendar, the phonebook, and SMS. BlueSnarf++ on the other hand is an enhancement of BlueSnarf with the ability of allowing full read and write access to the file system of the device.

Users of BT enabled devices should follow best practices, like turn off BT when not in use, restrict BT settings, remove trusted devices when no longer needed. However, BT devices should provide by default a safety barrier protecting their users, instead of relying on them to follow the best practices.

In fact, all the attacks affecting BT can be prevented by protecting the device from the RFCOMM protocol. Therefore, we proposed the design a BT Firewall for mobile phones. This feature will filter the RFCOMM connections and associate them by user and profile. By applying this sort of filter at the entry point of the connections, it will prevent BT attacks from being successful. The implementation of this BT Firewall and its evaluation are the tasks we intend to address in future work.

REFERENCES

[1] Global mobile statistics 2012: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats#subscribers. Last viewed 23.February.2012.

[2] Terrence OConnor, Douglas Reeves. Bluetooth Network-Based Misuse Detection. NC State University Raleigh. 2008 Annual Computer Security Applications Conference, 2008 IEEE.

[3] Alexander Gostev. Securelist, Bluetooth: London 2006. http://www.securelist.com/en/analysis?pubid=188833782. Last viewed 23.February.2012.

[4] BLUETOOTH SPECIFICATION Version 4.0 [Vol 0]. Master Table of Contents & Compliance Requirements. Publication date: 17 December 2009.

[5] Bluetooth Special Interest Group (SIG): https://www.bluetooth.org/. Last viewed 23.February.2012.

[6] Karen Scarfone, John Padgette. Guide to Bluetooth Security. National Institute of Standards and Technology. Special Publication 800-121. September 2008.

[7] A Gartner, Press Releases. Egham, UK, February 23, 2010. http://www.gartner.com/it/page.jsp?id=1306513. Last viewed 23.February.2012.

[8] Bluetooth: one billion devices and growing http://www.macworld.co.uk/digitallifestyle/news/?newsid=16477 Last viewed 17.February.2012.

[9] Bluetooth: 2 Billion In 2013 http://hothardware.com/News/InStat-Predicts-BluetoothEnabled-Device-Shipments-Will-Top-2-Billion-In-2013/. Last viewed 06.April.2012.

[10] Catherine Roseberry, About.com: http://mobileoffice.about.com/cs/traveladvice/qt/usingcellphone.htm. Last viewed 23.February.2012.

[11] Wireless and Mobile News. Mobile Apps Race to Serve Auto Market @IAA. 12.October.2009: http://www.wirelessandmobilenews.com/2009/10/mobile-apps-race-to-serve-auto-market-iaa-says-isuppli.html. Last viewed 23.February.2012

[12] Parrot, wireless devices for mobile phones: http://www.parrot.com/usa/. Last viewed 23.February.2012.

[13] Media Ford. Ford Teams up with Microsoft to deliver SYNC; In-car Digital System Exclusive to Ford. 7.January.2007: http://media.ford.com/Article_Display.Cfm?Article_Id=25168. Last viewed 23.February.2012.

[14] Andrew Y. Lindell. Attacks on the Pairing Protocol of Bluetooth v2.1. Aladdin Knowledge Systems and Bar-Ilan University, Israel. June 25, 2008.

[15] Trifinite Group: http://trifinite.org/trifinite_stuff.html. Last viewed 23.February.2012.

[16] Symantec. Symantec Report on the Underground Economy. Published November 2008.

[17] Lynn Tan, ZDNet. Symantec warns users over Bluetooth security. 21.September.2007: http://www.zdnet.com/news/symantec-warns-users-over-bluetooth-security/165841. Last viewed 23.February.2012.

[18] Don Reisinger, CNET. Bluejacking, bluesnarfing and other mobile woes. 22.August.2007: http://news.cnet.com/8301-13506_3-9764450-17.html. Last viewed 23.February.2012.

[19] Greg Kumparak, Mobile Crunch. Apple sold 8.75 million iPhones last quarter, 51.15 million since launch. 20.April.2010: http://www.mobilecrunch.com/2010/04/20/apple-q2-earnings-million-iphones. Last viewed 23.February.2012.

[20] NOKIA 30 GSM CONNECTIVITY TERMINAL AT COMMAND GUIDE, Issue 2.0. Copyright © Nokia 2002.

[21] Kevin Streff, Justin Haar. An Examination of Information Security in Mobile Banking Architectures. Dakota State University. Journal of Information Systems Applied Research. June 10, 2009.

[22] Proximity Marketing: http://www.bluetoothmarketing.com/. Last viewed 23.February.2012.

[23] Marketing Platform: http://www.breeze-tech.co.uk/. Last viewed 23.February.2012.

[24] JavaTM APIs for BluetoothTM Wireless Technology (JSR-82). Motorola Wireless Software, Applications & Services. 1.0a, April 5, 2002.

[25] Mohamed GHALLALI, Driss EL OUADGHIRI, Mohammad ESSAAIDI, Mohamed BOULMALF. Mobile Phones Security: The Spread of Malware via MMS and Bluetooth, Prevention Methods. MoMM2011, 5-7 December, 2011, Ho Chi Minh City, Vietnam.

[26] Yu Xin, Yan Ting. A Security Architecture Based on User Authentication of Bluetooth. College of Automation, Beijing Union University, Beijing 100101, China. © 2009 IEEE.